DATE: **26 April 1960**

NAME: **Friedman, William F.**

PLACE: **Breckinridge Hall, Marine Corp School**

TITLE: **Communications Intelligence and Security Presentation Given to Staff and Students; Introduction by probably General MILLER (NFI)**

Miller: ((TR NOTE: Introductory remarks are probably made by General Miller (NFI).)) Gentleman, I…as we've grown up, there have been many times, I suppose, when we've been inquisitive about means of communication, means of finding out what's going on. Some of us who grew up out in the country used to tap in on a country telephone line and we could find out what was going on that way—at least in the neighborhood. And then, of course, there were always a few that you'd read about in the newspaper who would carry this a little bit further and read some of your neighbor's mail by getting at it at the right time, and reading it and putting it back. Of course, a good many of those people ended up at a place called Fort Leavenworth.

This problem of security of information is with us in the military on a [sic] hour-to-hour basis because it's our bread and butter. It's what we focus on in the development of our combat plans in an attempt to project these plans onto an enemy and defeat him. And so, we use a good many devices. We spend a tremendous amount of effort and money in attempting to keep our secrets in fact secret—at least at the echelon where we feel this is necessary. Same time, of course, we always are interested in reading our enemy's mail or tuning in on his frequency and finding out what we can about him. We do this on a hourly basis. We do this in peacetime. And we increase the tempo in wartime.

Most of us here don't know much about how this is all accomplished. But we have a guest speaker today who has devoted his life to this business. He told me a while ago that forty years ago, he went to Washington as a lieutenant for a six-month's period of duty. And he's still there. ((Audience chuckles.)) Some of you who have just come from duty in the Pentagon or who have orders there now, shouldn't feel badly at all. ((More laughter heard.)) This is a great contrast to the devotion of a life—forty years—in this highly technical and professional field of communications intelligence. You all have had the biographical sketch issued which describes our guest speaker's background. And I'm sure you must be impressed, as I am, with this tremendous amount of personal devotion which this gentleman

has had…has made toward this one field of specialty. He has been recognized by our country, by our government. has been decorated for his services. holds a decoration that only one other person in our country holds—and this is significant.

It's with a good deal of pleasure that we have our guest speaker, who has come down here from Washington to be with us this morning and give us some of the highlights of what the problem is and how we solve part of our problem. Colonel William Friedman was here last year. I don't suppose there were two or three of the staff that are still here. So for us the material is fresh. Dr. Friedman…or Colonel Friedman, excuse me. ((TR NOTE: While the microphone is being adjusted, Mr. Miller addresses Dr. Friedman as follows:)) You can put this any place you want it…

Friedman: Yes.

Miller: Or just (B% kick) it around.

Friedman: Alright. Thank you very much. ((He pauses, then addresses the audience:)) General Miller, gentlemen. In inviting me to address the staff and students of the Senior School of the Marine Corps on the subject of communications intelligence and communications security, I assume that the objective is to make you aware of the roles that these two branches of the science of cryptology have played as vital military weapons in the past and may in the future again play.

Soon after the close of World War II, Service schools began asking for lecturers to tell their student officers something about our cryptologic activities during the war. There was at first serious question as to the advisability of lifting the security veil sufficiently to permit discussion of the subject. But in time, an affirmative decision was made. The official views of the Naval War College on the matter were stated in a letter dated 5 February 1946. And because that letter admirably states those views, I shall read two paragraphs of it.

In commenting upon the fine presentation made by a certain speaker, the letter said, quote—and this doesn't refer to me ((chuckling heard)): "His treatment of the subject matter emphasized the value of communication intelligence to naval commanders, the vital importance of maintaining the security of our own communication intelligence activities, and the necessity for observing the principles of communication security in defense against enemy communication intelligence. I consider that the value to be derived from the indoctrination of senior officers of the Navy in these principles far outweighs any possible loss of security resulting from a partial revelation of our activities in the past war, particularly in view of

the disclosures which have been made in the press." The letter continues, quote: "It appears axiomatic that the full benefit of communication intelligence can be obtained only when all senior officers realize its potentialities for winning and losing battles and wars, and when their actions are tempered by complete knowledge of the elements of communication intelligence rather than by *in*complete and *in*accurate information obtained through the channels of gossip." Unquote.

This being a TOP SECRET lecture, I will work up to that stage gradually. And I will begin by reading from a "BOTTOM" SECRET source which you all recognize. ((Audience laughs.)) I will preface the reading by reminding you that by that date, December the 17th, 1945, the hot war was all over. Or at least V-E and V-J days had been celebrated some months before. Many of you no doubt remember the loud clamor on the part of certain members of Congress who had for years been insisting upon learning the reasons why we were caught by surprise at Pearl Harbor. This clamor had to be met, for these Congressmen vociferously called attention to the fact that the war was over. And they contended that the truth could no longer be hushed up because of an alleged need for secrecy. They called for a real investigation, saying that although there had been investigations—a half a dozen or more of them—they wanted as a grand finale a joint Congressional investigation. They finally got what they demanded. The hearings disclosed many SECRET and TOP SECRET facts. And they also disclosed everything that had been said and shown at all the previous Army and Navy investigations. The Congressional hearings made headline copy for all of our newspapers.

There came a day in those hearings when the Chief of Staff of the United States Army at the time of the Pearl Harbor attack—five-star General George C. Marshall—was called to the witness stand. Toward the end of his ordeal, General Marshall was questioned about a letter he'd written to Governor Dewey during the heat of the 1944 presidential campaign. General Marshall pleaded long and most earnestly with the committee not to force him to disclose the letter or its contents because he said there was still a necessity for continued secrecy about code matters. But his pleas were of no avail. He had to bow to the will of the majority of the committee.

I will now read from *Time*. ((He pauses.)) "Pearl Harbor. 'Magic' was the word for it. U.S. citizens discovered last week that perhaps their most potent secret weapon of World War II was not radar, not the VT fuse, not the atom bomb, but a harmless little machine which cryptographers painstakingly constructed in a hidden room in Washington. With this machine—built after years of trial and error of inference and deduction—cryptographers had duplicated the decoding devices used in Tokyo.

Testimony before the Pearl Harbor Committee had already shown that the machine known in Army code as Magic was in use long before December 7th, 1941. Had given ample warning of the Japs' sneak attack, if only U.S. brass hats had been smart enough to realize it.

Now, General Marshall continued the story of Magic's magic. It had: 1) enabled a relatively small U.S. force to intercept a Jap invasion fleet; win a decisive victory in the Battle of the Coral Sea, thus saving Australia and New Zealand; 2) given the U.S. full advance information on the size of the Jap forces advancing on Midway; enabled the Navy to concentrate ships which otherwise might have been three thousand miles away, thus set up an ambush which proved to be the turning point victory of the Pacific war; 3) directed U.S. submarines unerringly to the sea lanes where Japanese convoys would be passing; 4) by decoding messages from Japan's Ambassador Oshima in Berlin often reporting interviews with Hitler, giving our forces invaluable information on German war plans. So priceless a possession was Magic that the U.S. High Command lived in constant fear that the Japs would discover the secret, change their code machinery, force U.S. cryptographers to start all over again." The *Time* article continues, but we'll come back to that perhaps later.

It is hardly necessary to tell you how carefully Magic was guarded before, during, and after the war. It is *still* very carefully guarded. Even the fact of its existence was known to only a very few persons at the time of Pearl Harbor—and that fact is an important element in any attempt to explain why we were caught by surprise. Now, I don't want to overemphasize the importance of COMINT in the Pearl Harbor disaster.

But as for its importance during World War II, I do want to tell you what General Chamberlain, who was General MacArthur's G3 throughout the war in the Pacific, has written about it. Quote: "The information given G2…ah…The information G2 gave G3 in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years." Unquote. Now, we can't put a dollar and cents value on what our possession of COMINT meant in the way of saving lives, but we can make a dollar and cents estimate of what COMINT meant by shortening the war by two years. A rough calculation tells us that each dollar spent for COMINT was worth…or the equivalent of one thousand dollars spent for other military activities. In short, when our commanders had COMINT, they were able to put what small forces they had at the right place and at the right time. But when they didn't have it—and this happened, too—their forces often took a beating.

Now, I hope I haven't tried your patience by such a lengthy preface to the real substance of my talk. So let's begin with a bit of background or

historical information about cryptology, which comprises two related sciences: namely, cryptography and cryptanalysis. They are but opposite faces of the same very valuable coin because progress in one inevitably leads to progress in the other. We could go far back into history and see the earliest beginnings of secret communications. And this might take us to the very dawn of the art of writing because there is room to wonder which came first—intelligible writing or unintelligible, that is, secret writing?

Instances of cipher are found in the Bible as this slide shows. In the Bible, Jeremiah, twice, there was this sentence involving the word "Sheshakh." For many years, it was not known what that word meant because there was no place of that name. But if you take the letters of the Hebrew alphabet and write the first eleven on one line and the second eleven on the other line, you set up a substitution alphabet by means of which the word "Sheshakh" is translated as "BBL: Babel ((or)) Babylon. Hebrew doesn't have any vowels.

And here's one historical item that is worthy of special notice: the scytale. Its earliest…It's the earliest cipher device history records. It was used by the ancient Greeks for military secrecy. They had a wooden cylinder of specific dimensions around which they wrapped spirally a piece of parchment. They then wrote the message across the edges of the parchment. You see that's not true in this slide. The translation there is wrong—I checked it myself. They then wrote the message across the edges of the parchment, unwound it, and sent it to its destination by courier where the recipient would align the parchment around an identically dimensioned cylinder. And thus bring together properly the bits of letters of the message.

It is interesting to note that the baton which the European field marshal still carries as one of the insignia of his high office derives from this very instrument. It is well known that Julius Caesar used cryptography—a very simple method—because all he did was to replace each letter by the one that was fourth from it in the alphabet.

The beginnings of modern cryptology can be traced back to the early days of the princes and chanceries of the Papal States, beginning even before the year 1300. Here's an alphabet of that period. It is interesting because it shows that even in those early days there already was a recognition of the basic weakness of what we call single or monoalphabetic substitution. Solution of this type of cipher, as you all know, is accomplished by take…by the fact that the letters in the alphabetic languages are used with greatly differing frequencies. This slide shows various equivalents…several equivalents for the high-frequency letters. They introduce stumbling blocks to solution by virtue of that fact. I will add that

the earliest tract that the world possesses on the subject of cryptology is that written in 1474 by a Neapolitan named Sicco Simonetta. He sets forth the principles and methods of solving ciphers in a very clear and concise form.

The first extensive treatise on cryptography is that by a German abbot named Trithemius, who wrote his monumental work in 1531. He planned to write four volumes, but he quit with the third because he wrote so obscurely and made such fantastic claims that he was charged with being in league with the devil. They burnt his books in fact, and his very life was in jeopardy. This may be a good place to present a slide of something from Trithemius which shows the necessity for secrecy in cryptology was recognized from the very earliest days. That's the oath which he suggested students be forced to take upon entering the subject of steganography; is an old term for cryptography or cryptology. We put teeth in our own somewhat similar oath, and here are the teeth. That's a special law to protect cryptologic secrets.

The next slide I show is a picture of what cryptographers usually call the Vigenère Square, by means of which polyalphabetic ciphers can be prepared. The square comprises a set of 26 alphabets successively displaced one letter per row. The plaintext letters are at the top, the key letters at the side, and the cipher letters inside. The method of using the table is to agree upon a keyword which causes the cipher equivalents of the plaintext letters to change according to the letters of the key. Vigenère described the square in 1586 and is commonly credited with having invented it. But he really didn't—and what's more, he never said he did. It was invented much earlier than 1586.

The next cryptographer I wish to mention is also a Frenchman—Francois Vieta, an eminent mathematician and founder of modern algebra. In 1589 when he was Councillor of Parliament at Tours and then Privy Councillor, he solved a Spanish cipher system using more than 500 characters so that all the Spanish dispatches falling into French hands were easily read. When Phillip II of Spain, who was absolutely convinced of the safety of his cipher, learned that the French were aware of the contents of his cipher dispatches to the Netherlands, he complained to the Pope that the French were using sorcery against him. Here's a slide that shows one of the hundreds of ciphers the Court of Spain was then using. Vieta was called upon the carpet and made to explain how he had solved the ciphers, otherwise "things" were going to "happen" to him.

I want to jump now to the period of the American Revolution. Believe it or not, the systems used by the Americans and by the British were almost identical. In fact, in one case, they used the same dictionary as a code.

For additional security, conventional words were used to represent the names of persons and places. Here are some of the codenames used by the British.

American generals took the names of the apostles. For example, Washington was James; Sullivan, Matthew; and so on. The names of cities: Philadelphia was Jerusalem; Detroit, Alexandria. The names of rivers and bays: the Delaware was the Red Sea; Susquehanna, the Jordan. Indians were called Pharisees and the Congress was referred to as the Synagogue.

There was an American who seems to have been the Revolution's one-man National Security Agency—for he was *the* cipher expert to Congress. And it is claimed he managed to decipher nearly all, if not all, of the British code messages intercepted by the Americans. Of course, the only way in which enemy messages could be obtained in those days was to seize couriers and take the messages from them by one means or another. Rough stuff compared to getting the material by radio intercept.

The next slide shows a picture of a code or syllabary, as we call it, used by Thomas Jefferson. This syllabary is constructed on the so-called two-part principle. You will note that the numerical groups are not in consecutive order, which means that you have to have a decoding section in which the code numbers are in numerical order, their meanings in random order. This sort of system even today is in extensive use but with larger vocabularies.

You've all learned as school children about Benedict Arnold and what he tried to do when he was Commanding General at West Point. You probably don't know that practically *all* his exchanges of communications with Sir Henry Clinton, Commander of the British Forces in America, were enciphered or in invisible inks. Here's an interesting slide showing one of Arnold's cipher messages. And right in the middle you'll see after the dash "If I" and then a code…a series of code numbers. Here is the translation. And it reads that he would give up West Point for the sum of 20,000 pounds, which he regarded as a quite nominal sum of money. Here's another in which he gave the British information which might have led to the capture of General Washington. But Washington was too smart to be ambushed. He went by a route other than the one he said he'd take.

I think you'll be interested to hear a bit more about that one-man NSA I mentioned a couple of moments ago. His name was James Lovell. Besides being a self-trained cryptographer, he was also a member of the Continental Congress, as I mentioned. There's on record a very interesting letter which he wrote to General Greene with a copy to General

Washington. I'll read it to you. "Philadelphia, September 21, 1780. Sir, you once sent some papers to Congress which no one about you could decipher. Should such be the case with some you have lately forwarded, I presume that the result of my pains herewith sent will be useful to you. I took the papers out of Congress and I do not think it necessary to let it be known what my success has been in the attempt. For it appears to me that the enemy make only such changes in their cipher when they meet with misfortune. And if there is no talk of discovery or…by me here or by your family, you may be in chance to draw benefit this campaign from my last night's watching. I am, sir, with much respect, your friend, James Lovell."

There's an episode which I learnt about only recently, and which is so amusing I must share it with you. It seems that a certain British secret agent in America was sent a letter in plain English, giving him his instructions. But the poor fellow was illiterate and had to call upon the good offices of a friend to read it to him. What he didn't know was that his friend was one of General Washington's own secret agents.

Before coming to the period of our Civil War—the war known by various names—I must mention Edgar Allen Poe who, in 1842 or thereabouts, kindled an interest in cryptography by his famous story of *The Gold Bug* and by some articles on cryptography in newspapers and journals of the period. For his day, he was perhaps the best informed person in the U.S. on cryptologic matters—though most of his source material came out of an encyclopedia.

The period of the Civil War, or the War Between the States, in U.S. history was as a result of the invention and development of telegraphy, a period in which the use of cryptography became very important. Here's a picture of a Confederate cipher device captured at Vicksburg. The device is a cylinder of wood covered with a sheet of paper bearing alphabets—the alphabets of that Vigenère table I showed you. There's a pointer. You could slide the pointer. There are two pointers, in fact. And you could turn the knob and bring about various alphabets according to key letters.

You might like to know two of the keywords that were used with this device for most of their communications. COMPLETE VICTORY was the first, The second was COME RETRIBUTION. Here's a picture of a message—authentic beyond question—sent by President Lincoln to General Burnside. If you read it as we normally do, it makes no sense. But if you read it backwards, it makes excellent sense. I think the President was kidding a bit, but he may have lacked confidence in the official crypto systems in the same way that during World War I, President Wilson lacked confidence in the codes of the State Department. I wish I

had time to show two or three slides of that part of President Wilson's time.

This is a photograph of a page or two from the codebook and cipher system used by the Federal Army. They had what we call "route ciphers"—that is they used diagrams of various dimensions and there were indications of the route to be followed in inscribing and transcribing the words of the message. The system was complicated by the use of arbitrary equivalents for the names of important people. President of the United States: Adam or Asia. Secretary of State: Abel, Austria. And so on. (B% And) the names of the famous generals of the Civil War.

I have with me today the complete set of cipher books used by the Federal Army during that period. I got that complete set, by the way, when an old Civil War veteran with whom I used to engage every few days conversation in the Wing 6, first floor of the Munitions Building. White-haired, fine gentleman. He came up to me one morning as I was coming into work, and he whispered, "They're burning things today." And I said, "Such as?" And he showed me these books. I said, "Would you mind lending them to me? I don't like to see them get burned. They belong to the archives of the United States." That's how I got them.

The next slide is a picture of a message sent to Grant in one of those route ciphers. "For U.S. Grant. No expedition to Texas (1-2G)." The words in the cipher message would be in disarranged order, taken from columns up and down.

After the Civil War, the use of cryptography in United States military affairs went into a decline because there was a long period of peace broken only briefly by the Spanish-American War. In 1885, the War Department published a code called "Code to Ensure the Secrecy of Telegrams." It is a cryptographic curiosity because the officer who was responsible for its production copied almost word-for-word the title page, the instructions for use, the arrangement of contents from a commercial code. And here it is. "The queen is the supreme power in the realm." Add any number below 25,000—say for instance 5555—to the numbers opposite to those words it is desired to transmit. So on. That's the left-hand part of the slide. The U.S. Army officer used not "The queen is the supreme power," but "or is a punishment whereof death is the maximum." Add any number. For instance, 3333—a great imagination/change from 5555. ((Audience laughs.)) This was the code that our Army used during the Spanish-American War. And in the copy I brought with me, there appears on the inside of the front cover the additive that was then used—777. Maybe they were rolling dice in those days.

In 1899, the Chief Signal Officer undertook the preparation of a suitable code for the Army. Economy was stressed. The Chief Signal Officer personally did all the work. ((TR NOTE: Dr. Friedman now addresses someone nearby, as follows:)) Sergeant, keep that last slide handy, will you? I'll come to it in a moment. Thank you. ((TR NOTE: Dr. Friedman returns to addressing the audience.)) And in 1902, the cipher of the War Department was published by the Adjutant General. In 1906, a revision of the book was published. And in 1915, a completely new code—the War Department Telegraph Code—was published. Believe it or not, that code was printed by a commercial printer in Cleveland. At least that's what my predecessor in the Office of the Chief Signal Officer told me when I took over from him after my World War I service in France.

During World War I, cryptology entered upon a new and rapid expansion in invention and development. With Hertz's discovery of the so-called Hertzian waves and Marconi's practical demonstration of signaling by wireless, a new era in military communications began. The first military usage of wireless, or radio as it soon came to be called in American terminology, was made in Europe before 1914. But wide usage of it began only in World War I. This brought our new developments in cryptography.

But before coming to these developments, a few words should be said about the U.S. position vis-a-vis the Allies and the central powers. Some of you well remember how President Wilson promised to keep the U.S. out of the war. How at one time during a period of strained relations with both sides, he declared that he'd never, never, never send our boys to war. He also said that there was such a thing as being too proud to fight.

This is a thesis I'll not try to defend. U.S. sympathies for the most part were with the Allies, especially the British. But there were in the U.S. millions of people who were against our entry into the war on either side—for there were times when British high-handed action almost precipitated us into the war on the side of Germany.

There were minor activities toward preparedness, but in the cryptologic field little was being done by either the Army or the Navy officially. Two Army officers became interested in the subject. And I'll show you the title page of the first American manual on military ciphers by the then Captain Parker Hitt. ((TR NOTE: He addresses the assistant:)) Sergeant, that was the slide that I asked you to put back. That's it. ((TR NOTE: He returns to talking to the audience.)) 1916, first edition. But this was almost a private venture despite the fact that it was printed at ((Fort)) Leavenworth ((Press)). Officially as regards cryptographic pub preparations, no new codes were being prepared in either service.

((Addressing his assistant:)) No, no, please. Double…When I press the button twice, you just turn off the lights. I mean, take off the slide. ((TR NOTE: He returns to addressing the audience:)) But this was…This thing of Hitt's was a private venture really. No new ciphers were being dreamed up. No cipher devices or cipher machines were being investigated or invented. As for cryptanalytic operations, well, there just were none whatever in either service—and for that matter, in the whole of the United States Government.

In a private research institution near Chicago—the Riverbank Laboratories of which I happened to be a member working in a totally different field of science—certain of us began studying cryptology. And soon, we began working on messages which were sent by…sent us by various government departments and agencies in Washington. Most of these were solved and returned to Washington. And my staff became more and more adept. But mind you, this was not even a quasi-governmental agency. It was operated as a patriotic gesture and at his own expense by the man who in 1915, '16—as an astute and wealthy businessman/colonel Kentucky variety/Colonel George Fabyan—foresaw the inevitable entry of the United States into the war. And he saw that the U.S. was wholly unprepared for any cryptologic work. The colonel was right. On 6 April, 1917, the U.S. almost suddenly, it seemed, declared war on Germany. How did this come about? It came about when it did as a result of a nice piece of cryptanalytic work by British cryptanalytic experts in London on a message now *world famous* as the Zimmerman Telegram. The message came from the German Foreign Minister in Berlin to the German Ambassador in Washington, who then sent it on to the German minister in Mexico City.

Here's the message in the form in which it was transmitted to Mexico. I won't go into the story about how the British solved it, but here's a translation of it. ((He pauses.)) As you can see, the Germans were going to resume unrestricted submarine warfare. But the part dealing with a proposal to be made to Mexico was the straw that broke the camel's back. People in the far…in the Middle West had been very lukewarm toward the idea of our getting into the war on either side largely because it was a war that was thousands of miles away. But when the Germans began talking about returning Texas, New Mexico and Arizona to Mexico, that was something else again. So we got into the war within a couple of weeks after the British gave us the Zimmerman Telegram. And we had established its authenticity. A year or so ago the telegram and the whole episode was the subject of one of the most dramatic episodes in Walter Cronkite's series of television programs, "You Are There." I wish I had the time to give you that here, but I don't. And a book of almost 250 pages dealing *only* with that telegram and episode was published just about a

year ago in our country, and just a few months ago in England.

Well, on 6 April, 1917, we were in the war as belligerents. And things began popping all over the U.S., including in my own little world at Riverbank Laboratories. We began training more people and doing more solution work, all paid for by Colonel Fabyan. We had solved many messages that dealt with our then not very friendly neighbor on our southern border, as well as messages that dealt with the activities of enemy agents. I'd like to tell you about one case, but I see the time is crowding up on me, and I'm going to skip that one. ((Dr. Friedman speaks to the person assisting him.)) Let's see the next slide, please. No, that's involved in that. I think we'll pass that. Makes a good story, but we have…just haven't got the time. That gives a little bit about the…how it was solved. Let's see the next one, Sergeant, please.

((Dr. Friedman resumes speaking to the audience. He pauses.)) The adjutant general began sending us officers for training. Here's a picture of one class—the biggest and the last one I directed before being commissioned and going directly to France. That picture spells out a message in cipher. You know, you get to a point in this business. ((Audience laughs; Dr. Friedman chuckles.)) Now that's Colonel Fabyan. Now that's Mrs. Friedman. These are two of my assistants. And that's yours truly. Now, the picture spells out the message…If this chap hadn't goofed ((audience laughs)) you'd never suspect that there was a cipher message. But the cipher is involved in whether the officers are facing straight forward or with their heads turned to either the left or the right. So that the message spells out "Knowledge is power." ((He pauses.))

Well ((he clears his throat))…Now for a quick look at the sort of things I found at GHQ in France when I got there and was assigned to work. Let's take first a look at some of the military crypto systems used by the various belligerents. Here's a picture of the system used…or rather *misused* by the Russians. It was based upon the old Vigenère principle using numbers instead of letters. Russian ineptitude in secret communications at that time cost them very heavily—for they lost the Battle of Tannenberg, a loss which greatly contributed to their being knocked out of the war.

The next slide shows a tactical cipher system used by the French. It was a transposition system—the columns being transcribed according to the columnar key. In addition, certain disturbing elements came into the method by taking the letters…taking off the letters in certain diagonals. And here is a picture of a system used by the Italian Army—again, only a variation of the old Vigenère system. Here is a system used by the Germans beginning in the latter part of 1917. It was invented by them. *Or* I should say they invented a clever combination of two methods. We

called it the ADFGVX cipher because the cipher text consisted exclusively of those letters. The final text as you see at the bottom contains only those letters: ADFGVX.

That system was a brand new thing in military cryptography and caused no end of headaches for the Allied cryptanalysts until it was discovered just how a solution could be achieved. The solution was not a general one, but depended upon special cases. However, these happened so often that we could bank upon them occurring practically every day. The ADFGVX system was used by the German High Command. And it wasn't long before it was discovered that if you made a study of only the number and direction of these messages, you could infer certain things about the tactical situation. And more important, you could with some degree of assurance predict what might happen in three or four days at a certain sector of the front. Here's an example of a chart based upon the ADFGVX intercept. This, gentlemen, represents an early, if not *the* first illustration in history of use of one of the basic principles of what we call traffic analysis and traffic intelligence. I wish I had the time to show you, but you can see—those up in front—how at the beginning of the Marne offensive the traffic went up very high and in various other places. We could bank upon that.

For tactical messages, the British and Americans employed a method known as the Playfair Cipher, which also uses a five-by-five…Oh, well, there's an example of some of the stuff that we would put out when the ADFGVX messages were solved. The next slide shows the Playfair Cipher. Uses a five-by-five square, by means of which not single letters but pairs of letters are enciphered.

In those days, the Playfair Cipher was regarded as pretty hot stuff. In fact, an officer of the American Army—the then Lieutenant Mauborgne, who later becomes Chief Signal Officer—wrote a little treatise published in 1914 in which he dealt with it under the title *An Advanced Problem in Cryptography and its Solution*. Today, our most elementary students are given things of that sort to solve after only a few lessons. The British Army developed a cipher device in World War I. They had manufactured a great many of them—thousands in fact. and they proposed to the French and to the Americans that all the Allies should use it for tactical communications. But for reasons that I'll tell you about in the last period, the device was never put to use. None of the belligerents in World War I used a cipher device or machine. So much for the military cipher systems in World War I.

Now I'd like to say a few words about the codes and code systems. A code is simply a sort of dictionary in which the words, phrases and

sentences are replaced by an arbitrary group of letters or figures. Codebooks are merely elaborations of the sort of syllabary that Jefferson used. Prior to World War I, the use of codebooks for tactical purposes was thought to be impracticable because of the danger of capture and the difficulties of compiling and reproducing and distributing new books constantly, especially under combat conditions. I don't think they thought too much about the possibilities of solving code. Early in 1916, the Germans began to use small field codes and the Allies soon followed suit. I had some slides to show of pictures of the pages of the codebooks, but I'll omit them and say that I brought exhibits with me. And you can see them after my presentation.

The only slide that I will show is one that will give you a picture of the Army…American Army's unpreparedness in World War I for secret communications. This is authentic. I didn't make it up because I found it in the records when I closed our office in the ADF in April of 1919. It's a code gotten out by the 52nd Infantry Brigade, dated 17 April, 1918. And it's what we may call "The Baseball Code." If you wanted to say "kill," you said "struck out." "Wounded" was represented by "hit by a pitched ball", and so forth. Very elementary.

In all that I've said thus far about our World War I communications, there's been little or nothing said about our high command ones—messages between General Pershing and Washington, for instance. For this, the Army had only the War Department Telegraph Code of 1915. It is with some sadness, but also with some amusement, that I tell you that soon after we joined the British, they told us with as much delicacy as you may imagine the situation required that our War Department Telegraph Code wasn't at all safe.

You don't have to wonder very much about the implications of such advice. But steps were taken right quickly to produce new and safer codes for the War Department and for high command use.

It was also about this time that our Navy began to improve its communications security by adopting a cipher device which went under the curious and almost movie-like title of ((said with emphasis)) "The NCB"—the Navy Cipher Box! And there is a picture of it. It was basically a modification of a very old device about which I'll tell you something later. I don't know what our State Department's communications security was like in those days, but I have my suspicions. The very old European tradition of secrecy and secret diplomacy was not our tradition. This was distinctly a European piece of "skullduggery"—and we wanted no part of it. Maybe our diplomats were taken for a cryptologic ride. I don't know. That would be something not for us today, but for some cryptologically-minded

historian to investigate in the voluminous records of our national archives. He might find some interesting things there. And here is a good point at which to bring to a close this first period devoted to old history.

The title of this period of my presentation might well be *The Influence of C Power on History*. Now, before any of you begin shouting "Yay, man" ((audience laughs)) or lest some of you jump to the conclusion that I've suddenly gone psychotic and am suffering from a delusion that I'm a reincarnation of the great Admiral Mahan, I hasten to explain that the "C" in that title is not the word "S-E-A" but the letter "C". And it stands for the word "Cryptologic." ((Audience laughs.)) The full title of this period of my presentation would therefore be *The Influence of Cryptologic Power on History*. As a subtitle, I would offer this: *Or How to Win Battles and Campaigns, and Go Down in History as a Great Tactician, Strategist, and Leader of Men.* Or on the other hand: *How to Lose Battles and Campaigns, and Go Down in History as an Incompetent Commander, a Military No Good-nich.* ((Audience laughs again.))

At this point let me hasten to deny that I'm casting any reflections upon certain spectacularly successful commanders. Names will occur to you without my specifying particular ones. In his recent book *Eisenhower: Captive Hero*, Marquis Childs says, quote, "Any examination of the relationship between Eisenhower and Marshall is handicapped by the fact that Marshall has never told his own story. Repeated efforts have been made to persuade him to write his account of the great events in which he played such a decisive part. He has replied more often than not that no honest history of any war has ever been written. And since he would not write unless he could tell the truth, he meant to keep silent." Unquote. I called Childs and I said, "You don't give any authority for that statement." He said, "Well, I was a guest twice at the Marshall home in Virginia and he told me twice what I had written."

Could it be that among other reasons why he held the belief that no honest history of any war has ever been written, General Marshall felt that if the COMINT facts were included in the history, the laurels of certain commanders on the winning side mightn't look so shiny as they generally appear? I'm here reminded of a story that came to me from a pretty reliable source a couple of years ago about a military man much in the current news. I think the story quite apropos in connection with what I've just said. It's about Monty ((Field Marshal Montgomery)). When Monty was in North Africa, he used to get these little bits of paper. Only Monty and his chief of staff knew about these bits of paper. Not even his G2.

One day, Monty had a meeting—prepare the events for the next few days. He outlined situations: what he thought Rommel was going to do; and

what dispositions he proposed. Some of the members of his staff were horrified. They tried to point out the weaknesses in Monty's estimate of the situation. Monty brushed them aside and said, "Gentlemen, make your dispositions accordingly. Dismissed." The next day, Monty got another piece of paper. Rommel had seen the weaknesses in *his* plan. Monty called his staff together and he said, "You know, gentlemen, I've been thinking over the objections that some of you have raised to my proposed plan. I think I was wrong. You were right." ((Audience chuckles.))

Sometimes, the course of history is materially changed by the amount and quality of COMINT that is available to field commanders and also how well they use it. Sometimes, it is materially changed by the absence of COMINT where it had been previously available and used. We have already noted one incident in which lots of first class COMINT was available—that which was available before the attack on Pearl Harbor. We may now take note of an incident of the second type, in which the consequences of the lack of COMINT played the most prominent role.

I have reference here to the Battle of Bulge, wherein a serious catastrophe was barely averted because our G2s had come to rely too heavily upon COMINT. So that when it was unavailable, they seemed to lack all information—or at least they acted that way. I said that a serious catastrophe was barely averted. But even so, the losses were quite severe. I won't go into them, but I have them here. What happened? Why? In an article entitled *Battlefield Intelligence: The Battle of the Bulge as a Case History* published in 1953 *Combat Forces Journal,* Hanson Baldwin said, quote, "Intelligence deficiencies and an astigmatic concentration upon our own plans with an almost contemptuous indifference for the enemies set the stage in December 1944 for the German successes in the Battle of the Bulge. A case history of the do's and don'ts of intelligence.

In General (B% Seibert's) words, we may have put too much reliance upon certain technical types of intelligence, such as signal intelligence"—that's another word for COMINT. "And we had too little faith in the benefits of aggressive and unremitting patrolling by combat troops. Dependence upon Magic or signal intercepts was major, particularly at higher echelons. When the Germans maintained radio silence, our sources of information were cut in half." Unquote.

There is hardly need for me to give you a definition of what used to be called Magic but is now referred to as COMINT. But perhaps I should cite its three principle objectives. First, to provide authentic information for policymakers to apprise them of the realities of the international situation;

of the war-making capabilities and vulnerabilities of foreign countries and of the intentions of those countries with respect to war. Second, to eliminate the element of surprise from an act of aggression by another country. Third, to provide the unique information essential to the successful prosecution and vital to a shortening of the period of hostilities.

It was in response to this last objective of COMINT that World War II gave a brilliant answer. I'm sure you would find the detailed story of the successes of the U.S. Army and the U.S. Navy cryptanalysts who worked on enemy messages in World War II very interesting. But there just isn't time enough to cite them in detail. I think the contents of the Marshall-Dewey letter, from which I read a bit in the first period, will have to suffice. However, in itself, it is sufficient to give you a pretty good idea of the contributions COMINT made toward our winning World War II. It is unfortunate that General Marshall's letter was disclosed during the Congressional hearings. For it's now in the public domain and its contents are undoubtedly known now to all the important chancelleries and the war offices of the world. General Marshall, remember, in his letter to Governor Dewey—sent during the political campaign of 1944—was asking Governor Dewey *not* to use certain information that Dewey got by surreptitious channels. We never learned how he got the information.

General Marshall gave some excellent illustrations of COMINT and its importance and why he was asking Dewey not to spill the beans. Quote: "Now, the point to the present dilemma is that we have gone ahead with this business of deciphering their codes"—Japanese codes—"until we possess other codes—German as well as Japanese. But our main basis of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin, reporting his interviews with Hitler and other officials to the Japanese government. They are still involved in the Pearl Harbor events." He meant that the same codes are still being used. Oshima was taken on a tour of the fortifications on the Atlantic seaboard in France. As soon as he got home, he sent his notes to Tokyo. We read those. General Eisenhower knew every emplacement.

I'll go on with General Marshall's letter: "To explain further the critical nature of this setup which would be wiped out almost in an instant if the least suspicion were aroused regarding it, the Battle of the Coral Sea was based on deciphered messages. And therefore our few ships were in the right place at the right time. Further, we were able to concentrate our limited forces to meet their advances on Midway, when they otherwise would certainly have been some 3,000 miles out of place. We had full information of the strength of their forces in that advance, and also of the forces directed against the Aleutians, which finally landed troops on Attu and Kiska. Operations in the Pacific are largely guided by the information

we obtain of Japanese deployments. We know their strength in various garrisons, their rations, and other stores available to them. And what is of vast importance, we check their fleet movements and the movements of their convoys." Matter of fact, we had better logistical information than the Japanese themselves had in Tokyo.

"The heavy losses reported from time to time, which they sustained by reason of our submarine action, largely results from the fact that we know the sailing dates and the routes of their convoys—and can notify our submarines to lie in wait at the proper point. The current raids by Admiral Halsey's carrier forces on Japanese shipping in Manila Bay and elsewhere were largely based in timing on the known movements of Japanese convoys—two of which were caught as anticipated in his destructive attacks. The conduct of General Eisenhower's campaign and of all operations in the Pacific are closely related in conception and timing to the information we secretly obtained through these intercepted codes. They contribute greatly to the victory and tremendously to the savings of American lives—both in the conduct of current operations and in looking toward the early termination of the war." Unquote. Dewey was a real patriotic American citizen. He never breathed a word in his campaign.

It will be helpful to list in sequence the steps involved in the production of COMINT. First, of course, comes intercept. You've got to have the traffic. And getting it is no small trick. Modern electrical high-speed communication systems used by large governments require high-class intercept operations. The interception of traffic is not only a complicated, but also a very expensive enterprise—costly in numbers of personnel and equipment. If there were time, I'd show a few slides of typical intercept stations and intercept positions. You must realize surely that the business of intercepting a message is hardly identical with that of receiving a message when the transmitting and receiving operators are legitimate members of the same radio net. The intercept operator may be located hundreds or even thousands of miles away. And he can hardly break in and say, "Hey, bud, I didn't get that last group. Repeat it, please." ((Audience chuckles.))

Getting the intercept copy back to where it can be worked on—that is, getting it there in good time—is also complicated and highly important. Much of the traffic has to be forwarded electrically which requires the armed forces to allocate special communications channels and facilities for this purpose. Speedy communications is therefore an extremely important factor and perhaps the real key to success in the production of COMINT. ((He coughs.)) The excellence of our communication systems is a very important factor. Unless we can get the traffic quickly and accurately back to where it can be worked on by the analyst, and unless

we have rapid and secure communications to the various analytical stations and also to those authorized to receive the final COMINT product, you're conducting a mere exercise—not a real operation.

The next step after interception is traffic analysis—that is, the reconstruction of the radio nets of the enemy and the identification and location of their transmitting stations. This gives very important information on two counts. First of all, establishing or reconstructing the nets gives you order of battle. The reconstruction of radio networks is not easy when the callsigns and frequencies are changed rapidly. It is a striking fact that all through World War II the enemy was able to change callsigns and frequencies apparently without too much trouble. These changes gave us a good deal of trouble, and we had to keep many people working on this phase of intercept operations all the time.

The second good reason for engaging in traffic analysis is that every once in a while your cryptanalysts come up against a road block, and they can't produce any COMINT—in which case the only thing you have to fall back upon are non-COMINT sources of information. But you can still get good information from traffic analysis from simply watching the ebb and flow of traffic, changes in routings: from which you can make inferences of what is happening or is going to happen. Now these, mind you, gentlemen, are only good guesses and they might be wrong. The stories they tell aren't always reliable, and you have to be very careful sometimes in acting upon them. They're not like decrypts, as we call them—(B% meaning) bits of paper. Those decrypts come straight out of the horse's mouth.

The next step, of course, is cryptanalysis, which yields what we call decrypts: the raw information upon which COMINT is based. It is obvious that the decrypts, if they are in a foreign language, have to be translated into good English. And with the translation, there's always a certain amount of emendation because of errors in transmission, reception, errors made by cipher clerks and so on. You must bear in mind that all this business is conducted as a very large-scale production or exploitation operation. You're not dealing with just a few messages a day. There are thousands of them!

The next step is the evaluation of the information. And please note that I refer to the decrypts not as COMINT, but as raw products. That is something which the intelligence people are most insistent about saying that it's their job to evaluate the decrypts and to collate and check the information they yield against information from other sources. And I suppose this is reasonable and necessary. It is conceivable that an astute enemy might actually mislead you by sending out a phony or two, in which case the intelligence people should be able to detect the spurious

message by collating what it says with what there is from other sources.

And there, then, comes finally the dissemination of the COMINT product/ And this has to be very, very carefully controlled. For this purpose, there are special crypto systems and special security officers. And the decrypts are kept out of the normal communication centers or message centers so as to keep the number of persons authorized to receive COMINT to an absolute minimum. All these persons have to have a very special clearance. I won't even name it.

Now I'll go back to the COMINT processing and give you a bit of information about cryptanalytic techniques and gadgetry. I venture to say that you all know the sort of mental picture the average citizen has of a cryptanalyst. He's a long-haired egghead. Has long whiskers with crumbs in them. He has grimy fingers and grimy fingernails. And he wears thick spectacles when at work. This chap is supposed to go into a huddle all by himself with a cryptogram. And sooner or later he comes up with the answer shouting, "Eureka!" ((Audience chuckles.)) Well, that picture is far from the truth these days. For cryptology is big business now—very big business indeed. I won't tell you ((he pauses))…Oh, what the hell! ((Audience chuckles.)) It's costing us a half a billion dollars a year, maybe more.

Cryptanalysis of modern crypto systems has been facilitated, if not made possible, by the use and application of special cryptanalytic aids—including the so-called electronic brains. That is, high-speed electronic machinery and digital computers. Some are standard machines, but mostly we devise modifications of them. At this point, I must take a few moments to clarify the picture and in simple language tell you what such gadgets do for us. Attacks on good, modern cryptosystems usually involve making a great multiplicity of hypotheses, each of which must be tested out one after the other until you find a correct one. The job of the cryptanalyst is to devise shortcuts for testing these hypotheses. The shortcuts are often based upon the use of statistics and statistical theories having to do with the relative frequencies of letters, pairs or sets of letters, words, sets of words, and so on.

Having devised the proper tests: of course human labor could be set to work making the millions of tests in order to find the correct hypothesis or to cast out the vast majority of incorrect ones. But it is obvious that you would have to have, as we used to say in the old days, "factorial (B% in Chinamen") to do the job—or else the job would take eons of time. Now it is our experience that in most cases, it is practical to build machines which will make the tests. I don't have to tell you that machines don't tire as rapidly as humans. They don't need sleep or time out for meals, or for

recreation, or for such things as shopping, lovemaking and so forth. ((Audience laughs.)) In short, the care and feeding of electrical machines is a relatively more simple matter than the care and feeding of human beings. But basically, these machines can only do one thing: they can perform at a high rate of speed processes which the human brain and hand can perform, but only at a much slower rate. Let me emphasize that these machines *don't*…They *cannot* replace the thinking processes involved in cryptanalysis.

This may be at a very good place to read a paragraph or two from a recently published book by retired four-star General Albert C. Wedemeyer to show you what misconceptions about cryptology can be entertained even at the highest levels when the information comes—as the Navy letter I read you at the beginning of the first period—via channels of gossip. General Wedemeyer states in connection with his discussion of U.S. culpability in the Japanese attack on Pearl Harbor that President Roosevelt had ample time to broadcast the warning. And he goes on to say, quote, "The argument has been made that we could not afford to let the Japanese know we had broken their code. But this argument against the Presidential warning does not hold water. It was not a mere matter of having broken a specific code. What we had done was to devise a machine which could break any code, provided it was fed the right combinations by our extremely able and gifted cryptographers." I bow. ((Audience laughs.)) "The Japanese kept changing their codes throughout the war anyway. And we kept breaking them almost as a matter of routine." Unquote.

Would that we had had such a machine then or that we had it now. For it would do what no machine can yet do so far as I'm aware: namely, think even simple thoughts. When I read that passage in Wedemeyer's book, next time I went out to see my friend at NSA, I said, "Boy, you're holding out on me. Come across!" ((Audience laughs.)) Oh, I know that certain large and complex electronic digital computers can do things which almost resemble thinking processes. (B% There), for example, play chess. But the resemblance, even though close, is a far cry from what the human brain does in playing chess. You can program a machine to make three moves, four moves. After that, nothing.

I'd like to show you what some of our latest and most sophisticated and highly specialized machines look like. But I'm sorry that I can't do so, even in a TOP SECRET lecture—even before you, each one of you holding a TOP SECRET clearance. It's simply that our special regulations won't permit me to do so. If there's time at the end of this period, I'll show you some of the World War II ones perhaps. ((Audience chuckles.))

Because of the complexities of modern high-grade crypto systems, the great majority of them cannot be solved in the field—either at the intercept site or a rear headquarters. Cryptanalysis of some low-rate systems and a certain amount of traffic analysis *can* be performed by field units to meet certain immediate needs of field or base commands or forces afloat. Each service provides for its own special needs in field processing. But COMINT processing is essentially a complex activity, and much of it can be done well only at major processing centers where the limited numbers of highly skilled personnel can be concentrated and very specialized analytic machinery can be installed. But it's not enough merely to install them. They have to be maintained, and that's not easy. This air conditioner, for example. ((Audience laughs; he chuckles.)) There is no pool in civil occupations for cryptanalytic machinery engineering and maintenance personnel. This is an important fact to remember. We've got to train our own in pretty nearly all cases.

I want to say a few words about the great importance of coordinating COMINT activities with other intelligence operations and with a tactical situation. Although COMINT is the most reliable, the most timely, and in the long run the most inexpensive kind of intelligence—inexpensive in terms of lives—it must, as I've said before, still be evaluated, collated, correlated, and coordinated with intelligence coming from other sources, if for only this reason: to provide data for cover and protection of COMINT sources. When a decision has been made to take action based upon COMINT, careful efforts must be made to ensure that the action cannot be attributed to COMINT. This is very, very important. When possible, action must always be preceded by suitable reconnaissance and other deceptive measures. Otherwise, the goose that lays the golden eggs will be killed.

I'm going to give you one example of what is meant by COMINT cover. On a certain day in November 1944 an enciphered code message was sent by a certain Japanese staff section to a certain Japanese Air Force unit requesting air escort for two convoys carrying troops to reinforce the Philippines. The message gave the number of ships, tankers, escort vessels, date of departure, port, and route, and new positions for the next seven days. The message was solved in Washington. Two days after the convoy left, one convoy commander reported in a message—which was also intercepted and read—that his convoy had been sighted by a B-29 with strong indications that the other convoy had also been sighted.

A few hours later, messages from these convoys reported losses as follows. Six ships definitely sunk; one disabled; one on fire. Later, we learned from another source that one aircraft carrier was also sunk. But did you notice that message about the B-29? That B-29 just didn't happen to be cruising around there. It was sent there to be observed. That was

good COMINT cover.

Of course, knowledge and experience point to the necessity of exploiting every possible advantage a tactical situation affords. And the temptation is naturally very great in the heat of battle to use COMINT whenever and wherever it is available. This may lead to carelessness which quickly jeopardizes COMINT sources. Of course, the full value of COMINT cannot be realized unless operational use is made of it. However, when action based on it is contemplated, possible compromise of source must always be borne in mind and the danger of compromise weighed against the military advantages to be gained. A minor military advantage is never alone sufficient grounds for risking the loss of this source. This is a cardinal principle in continuing COMINT success.

Also, we must bear in mind that crypto systems are usually worldwide or area-wide in distribution. And changes made as a result of suspicion of compromise in one area may therefore have a far-reaching consequence on the ability to produce COMINT elsewhere. The commander seeking a minor advantage by using COMINT in one locality, may thus deprive another commander of much greater advantage—or even deny it to the commander of a major operation.

Finally there is another aspect of coordination. It's that between the operation officers and the COMINT officers. The COMINT authorities should be carefully oriented to give the optimum coverage for operations and progress. Only very limited numbers of centers, facilities and personnel are available. And only a part of the enormous amount of traffic can be obtained and processed. Therefore, it is essential that COMINT producers be constantly informed of current and planned operations so as to direct attention where most is needed. This is a very important point to get across. It is difficult because commanders in charge of large-scale operations are naturally leery of telling any outsiders what they are planning to do—and how, when, and where. Mutual confidence must be established, however, so that the COMINT producers learn what the commanders are planning. They support one another.

There isn't…This isn't the only or most important kind of cooperation that is absolutely vital for success in COMINT production, which nowadays is done on a worldwide scale and requires a great deal of cooperation of all sorts among many thousands of skilled personnel scattered practically over much of the earth's surface and separated by hundreds or thousands of miles. The integration and direction of the COMINT effort is a truly huge military enterprise and requires a high order of managerial ability and intelligence.

Let me close this part of my presentation by saying that not only does NSA have a large number of workers in COMINT endowed with great intellectual capacity—I can say that because I'm not actively engaged in it now ((audience chuckles))—but it also has available to it and uses the brains of some of the greatest scientists of our country. They come as consultants and advisors. They're members of our board. They work on NSA contracts. And they help NSA in other ways—for example, by moral support when it comes to reaching into high places in government for money and people.

This ends the COMINT portion of my presentation, and in the next and final period, we'll devote our attention to COMSEC. Now, I said that if there were a few minutes I might show you a few things of World War II days. So let's have the first slide. Oh, that's the picture that the average person has of the cryptanalyst, you see? I described him to you. ((Audience chuckles.)) When he gets going real good, he may get himself an assistant. There, you see? And I see all the keys labeled. He's got himself an assistant. That's a breadboard model of a WM. ((Audience laughs.))

I told you that there were thousands of messages. This is the average daily volume, period 1941 to the end of 1945—the end of hostilities. Thousands. And there were a thousand and one hundred in one month in 1945. Everybody talks about *the* Japanese code, *the* German code, *the* Navy code. There is no such thing as "*the"*! The number of cryptographic systems in effect in the U.S. Army *alone* in the period 1941-45: seven hundred…over seven hundred in simultaneous use.

Oh, a picture of one of our World War II gadgets: a modified IBM machinery. It looks rather messy to me nowadays, but I tell you it looked beautiful in those days. Oh! ((Audience laughs.)) I may have used the "beautiful" in the wrong slide. This gal is working a machine that was deciphering Japanese military attaché messages in a very complex system. But there's the machinery for the solution. She punches the keys and the answer comes out here. It's another machine that was modified—IBM. Still another one. This did special searching at a very high rate of speed.

There's just one section of two or three wings in the old building at Arlington Hall filled with IBM machinery. We had the largest IBM installation in the world. ((He pauses.)) I'll whisper this: that's our version of the Japanese so-called Purple—the one involved in the Magic…of the Japanese Foreign Office communications. ((TR NOTE: This was not whispered.)) We never saw the original. This was all constructed from pure analysis. The only machine that we did see was a burnt and

blackened piece of apparatus taken from the basement of the Japanese embassy in Berlin after hostilities had ended. I won't try to explain this thinking.

Several years ago, there was being hammered into our ears over the radio in Washington a slogan concerned with automobile traffic safety. The slogan was: "Don't learn your traffic laws by accident." I think the slogan useful as a subtitle for this last part of my presentation, which is devoted to communications security. But I'll modify the slogan a little bit: "Don't learn your COMSEC laws by accident." I know, of course, that only a few of you will ever be directly concerned with COMSEC duties, but as potential future commanders of fighting units, a dictionary definition of the word "accident" should be of interest in connection with a story I shall tell you in a moment or two after I've read Webster's definition. If you'll bear with me. "Accident: literally a befalling. An event which takes place without one's foresight or expectation. An undesigned, sudden, and unexpected event. Hence, often of an undesigned or *unforeseen* occurrence of an afflictive or unfortunate character. A mishap resulting in injury to a person or damage to a thing. A casualty, as to die by accident."

I will now make the definition relevant by reminding you of a minor but nevertheless quite important episode in the Pacific during World War II. I will preface the account of that episode by reminding you that during our participation in World War II, the President of the United States, accompanied by a good many VIPs, journeyed several times halfway around the world to attend special conferences. They apparently could go with safety almost anywhere. They met with no accidents. On the other hand, the Japanese Commander in Chief of the Combined Fleet, Admiral Yamamoto, went on an inspection trip in April, 1943—the sequel to which may be summarized by an official Japanese Navy communiqué reading in part as follows. Quote: "The Commander in Chief of the Combined Fleet, Admiral Yamamoto, died an heroic death in April of this year in air combat with the enemy while directing operations from a forward position." Unquote. I'm sure that everybody in this audience knows that Yamamoto didn't die in air combat with the enemy while directing operations. He met with an accident. ((Audience laughs.))

I don't know who first used the following terse statement, but it is decidedly applicable in this case: "Accidents don't happen. They are brought about." In the case of Yamamoto's inspection trip, our Navy had his schedule in detail down to the very day, hour and minute. They also knew what his air escort would be. It was relatively easy to bring about the "accident" Yamamoto was to suffer. His death was no accident in the dictionary sense of the word. It was brought about because his communications were not secure. The Yamamoto incident later gave rise

to a somewhat amusing exchange of TOP SECRET telegrams between Tokyo and Washington. And after the war was all over, certain of them turned up in the Forrestal diaries, from which I will now read. Quote: "The formal surrender took place on the deck of the *USS Missouri* off Tokyo Bay on September 2nd."

"The mood of sudden relief from long and breaking tension is exemplified by an amusing exchange a few days later of urgent TOP SECRET telegrams which Forrestal put in his diary. In the enthusiasm of victory, someone let out the story of how in 1943 Admiral Yamamoto, the Japanese Naval Commander-in-Chief and architect of the Pearl Harbor attack, had been intercepted and shot down in flames as the result of the American ability to read the Japanese codes. It was the first public revelation of the work of the cryptanalytic division. And it brought an anguished cable from the intelligence unit already engaged at Yokohama in the interrogation of Japanese naval officers. The cable said, subquote, 'Yamamoto's story in this morning's paper has placed our activities in a very difficult position. Have meticulously concealed our special knowledge. We now become ridiculous.'"

At this point, Forrestal interpolated that, quote, "They were even then questioning the Japanese officer who had been responsible for these codes. And he was hinting that in the face of this disclosure, he would have to commit *hara-kiri*." The cable continued: "This officer is giving us valuable information on Japanese crypto systems and channels. And we do not want him or any of our other promising prospects to commit suicide until after next week when we ((audience laughs))…we expect to have milked them dry." Unquote. Washington answered with an operational priority TOP SECRET dispatch. Quote: "Your lineal position on the list of those who are embarrassed by the Yamamoto story is 5,692. ((Loud audience laughter.)) All the people over whose dead bodies the story was going to be published have been buried. All possible schemes to localize the damage have been considered, but none appears workable. Suggest that only course for you is to deny knowledge of the story and say you do not understand how such a fantastic tale could have been invented. This might keep your friend happy until suicide time next week—which is about all that can be expected." ((More laughter from audience.))

But not many years passed before the Japanese began to realize the truth. And recently published books by Japanese naval officers come out quite openly with statements attributing their defeat to poor COMSEC on their part and excellent American COMINT and COMSEC. For example, I'll read you a paragraph from Captain Fuchida's book entitled *Midway: The Battle that Doomed Japan*. Quote: "If Admiral Yamamoto and his staff were vaguely disturbed by persistent bad weather and by lack of

information concerning the doings of the enemy, they would have been truly dismayed had they known the actual enemy situation. Post-war American accounts make it clear that the United States Pacific Fleet knew of the Japanese plan to invade Midway *even* before our forces had started from home waters. As a result of some amazing achievements of American intelligence, the enemy had succeeded in breaking the principle code then in use by the Japanese Navy. In this way the enemy was able to learn of our intentions almost as quickly as we had determined them ourselves." Unquote. Matter of fact, Admiral ((Joseph)) Wenger told me—who was engaged in the Navy cryptanalytic operations for a good many years; very good friend—told me that at the time of the Midway messages being solved, the results were placed before the Navy High Command out there. And they were very, very dubious about taking advantage. They said, "What? Shall we rely upon what some young squirts have worked out or say they got?"

So much for an introduction to this period on COMSEC. And now let's get down to the matter itself. It's hardly necessary to tell you that with the advances made in the invention and development of various weapons of warfare—including communication systems—the old so-called pencil and paper ciphers, the hand-operated small cipher devices, and the codes of former days became completely inadequate. Military naval and air secret communications had to be speeded up. And obviously the best way to produce the necessary improvements lay in the development of crypto apparatus by means of which speed in crypto communications would at least begin to approach the ever increasing speed of electrical communications. And let me remind you that the impetus for devising and developing their means for crypto communications came not only from the need for speedier crypto apparatus, but also—and perhaps more importantly—from the need for much greater security in those communications, which were now largely by radio and were therefore susceptible of interception and study by the enemy. Greater security was needed because cryptanalysis had been made much more effective by advances in that time aided by new cryptanalytic tools.

A brief history of the invention and development of crypto apparatus will therefore be of some interest. We shall proceed now with some slides. Aside from the much earlier scytale used by the ancient Greeks, the earliest cipher device known to history is the cipher disk first described by an Italian cryptographer named Alberti who wrote a treatise on ciphers in Rome about 1470. The next slide shows a similar sort of wheel which appeared many years later in a book by another Italian cryptographer, Porta, who recommends the use of the cipher disk with keywords. I brought the Porta book with me. The next slide pictures the U.S. Army cipher disk which was used in the period 1914-1918 and which follows

exactly the same principles that Alberti recommended. Seems to have taken a long time for the Signal Corps to get caught up with Alberti. ((Audience chuckles.)) Now, I know it takes a long time to nurse a patent through the Patent Office, but Alberti's device was finally patented in 1924. Here it is. ((Audience laughs.))

Next is a picture of the Wheatstone cryptograph, the first real improvement on Alberti's device. I have and brought with me the only original in the United States, maybe in the world. Sir Charles interested himself in cryptography and invented his device in the latter part of the decade 1870. It consists of an ordinary alphabet on the outside and a mixed alphabet on the inside. But there is one additional and important feature: the alphabet on the outside contains 27 places; the one on the inside, 26. There is differential gear in the device so that as you encipher a message and turn the bigger minute hand to the letters of the plaintext, the small or hour hand advances one step for each complete revolution of the minute hand—just as in a clock. Thus, the cipher equivalents change as you go round and round. And the music comes out here. ((Audience chuckles.))

In 1917, in casting about for a field cipher device for use on the Western Front, our British allies resuscitated Wheatstone's principle, embodied it in a little different mechanical form, and made thousands of them. Here is one of them. And I have also with me a copy of our model. It has a 27-unit alphabet on the outside and a 26-unit on the inside. But there's now one additional and very important feature. You'll notice that both alphabets can now be made variable mixed sequences—whereas before in the original Wheatstone only the inner alphabet could be varied. Now, a good many of these devices were just about to be issued to field units—not only British, but also French and American. All the top cryptographers of the Allied Forces were sure of the crypto security of the device. But even before they could be put into use, it was shown by a young upstart still wet behind the ears that its security wasn't what those cryptographers thought it was.

I was still at Riverbank when I proved its insecurity by solving five short messages sent to Riverbank as a challenge. The first message said, "This cipher is absolutely indecipherable." ((Audience laughs.)) When I reached American GHQ in France about three months later, I found I wasn't a bit popular because those thousands of Wheatstone devices which had been issued had to be withdrawn even before they could be put into use. Reliance therefore continued to be placed in codes.

Sometime in the 1890s, a French Army reservist, Commandant Bazeries, tried to interest the French Army in a device which he called a *Cryptographe Cylindrique*—or cylindrical cipher. His device consisted of a

series of disks with a central hole so that they could be mounted upon a shaft. Each disk bears an alphabet—25 letters in this case. This arranged. And the mixed alphabets were all different. Each bearing an identifying letter or number for assembling them upon the shaft in some key order so the correspondents have the same sequence of disks on their cylinders. You encipher your message twenty letters at a time—as there are twenty rings—by rotating the rings to align the letters of your plaintext horizontally. Whereupon, for the cipher text ,you can choose any one of the other 24 rows of cipher text. This principle seemed a very good one. You see that middle line: "JE SUIS INDÉCHIFFRABLE." Then you could take for your cipher any of the other lines. Then you've set up your next twenty letters. This principle seemed to be a very good one, and messages in it appeared to be quite safe. But Bazeries never got anywhere in his attempts to get the French Army to adopt any of these ciphers, including the cylindrical cipher.

In 1915, an American Army officer Captain Parker Hitt, whom I've mentioned before—there he is; still living—conceived the crypto principle of the cipher cylinder independently. He knew nothing about Bazeries. His device, however, took the form of strips as you can see. This was Hitt's very first crude shot at it. And I have the original as a gift. It's one of the very interesting items in my private collection. Here's a better model also made in 1915 by Hitt with paper strips mounted upon wood…wooden sliders. That device was brought to the attention of the then U.S. Army Signal Corps Major Mauborgne—later became Chief Signal Officer—who imagined he'd thought up something new when he made a cylindrical form of the thing going back unknowingly to Bazeries' model. Here's Mauborgne's model. It's made…The original was made of brass and was very heavy. I brought it with me. Here's the final form of the device as adopted in 1922 by the U.S. Army. It became what we call Cipher Device, Type M-94. And it was used by the Army, the Navy, the Coast Guard, and Treasury.

A couple of years ago…A couple of years after the M-94 was put into service, I came across a write-up in the Library of Congress among the papers of Thomas Jefferson. Jefferson was the first to invent the cipher cylinder principle. He anticipated the Frenchman Bazeries by a century! Here is the first page of his description of the device which he called *The Wheel Cypher*. Here's the second page. At the bottom, you can see his calculations—the number of permutations you can get.

In studying the degree of security provided by the M-94, both Army and Navy cryptologists soon came to the conclusion that security would be much increased by the use of changeable or variable instead of fixed alphabets. Among other versions, I had made one which used metal rings

in which you could mount slips of paper and fasten them. Thus we could change the alphabets as often as necessary. Navy tried other versions. Between Army and Navy, the various forms of strip cipher devices were developed and came to be used by the armed forces—and later by the State Department and the Treasury Department. Here's a picture of the final U.S. Army Strip Cipher Device called an M-138A. The strip ciphers carried an enormous amount of traffic before and during World War II. But there were…But they were so-called hand-operated or pencil and paper ciphers. Whereas what we *needed* were machines or better devices.

First, let's see a machine called the Kryha invented by a German in about the year 1925. According to its inventor Kryha, it was the last word in the way of mechanical cryptographs. And he tried to interest various governments in his machine. There isn't time to explain it, but here's a dissertation on the number of permutations and combinations the Kryha machine affords written by German mathematicians. All I have to say about it is that in this case, as in many others, merely the number of permutations and combinations which a given machine affords, like the birdies that sing in the spring, often have nothing or little to do with the case. Much depends upon just what kinds of alphabets are employed and exactly how they are derived. And various other factors are involved.

Large numbers of permutations and combinations don't frighten the cryptanalyst at all. For example, to give you a simple illustration, take a simple monoalphabetic substitution cipher. The number of alphabets that can be produced is factorial 26. That's a large number. I'll read it to you: "Four hundred and three quadrillions, two-hundred and ninety-one thousand four-hundred and fifty-one trillions, one-hundred and twenty-six thousand six-hundred and five billions, six-hundred and thirty-five thousand five hundred and eighty-four millions, and a few more. But you know as well as I that you don't solve monoalphabetic substitution ciphers by the exhaustion method. There are very much simpler ways of solving them.

In our various attempts to develop better crypto machines, it became clear that there was pressing need in the military and naval services for two types of automatic machines. First, we needed a small, preferably mechanical machine for low echelon or field use. And second, we needed a larger electrically-operated machine for high security, high command use. Let's take up the first of these two types and see what happened. Here's a machine constructed by the Signal Corps laboratories about 1934 without guidance from Washington. The director of the laboratories at that time was a great believer in autonomy, and he wasn't going to have Washington tell him anything about how things were to be done in his laboratories. When it came to develop…to developing a cipher machine,

he decided that he and his staff could produce a really good machine without the help of Washington cryptanalysts.

So he proceeded on this basis to use up the tiny bit of money that was then available—two thousand dollars! We in Washington were not permitted even to know what was being built until the final model was completed and ready to be delivered to us. When we finally went to pick up the machine, I talked to Colonel So-and-so who told me with some pride that his machine was all mechanical and that there was nothing in the way of an electrical machine or operation that you couldn't do mechanically. I asked, "Colonel, can you light a room mechanically?"—to which he replied, "You've said enough. Get out! There's the machine. Take it with you." The colonel never was given the opportunity to improve his model because the crypto principle was so faulty that we solved test messages in twenty minutes. The laboratory development came to a sudden and inglorious end. ((Audience laughs.)) That fiasco wasted what little money we had for such business.

Now, we come to a development which is of considerable interest to us. Here's a picture of a gentleman named Boris Caesar Wilhelm Hagelin, a Swedish engineer who was responsible for the invention and development of one of the machines that all the American field forces used in World War II in great quantities. I was opposed to adopting Hagelin's device and I'm positive it wasn't a case of NIH—"Not Invented Here" factor. The decision to adopt them was made about 1939 at a level much higher than my own. And it turned out that my superiors were right. For our troops at least had something for low echelon crypto communications. Whereas, if I had had my way, they would have had nothing but pencil and paper ciphers, or the M-94 device, or the strip cipher device—all of which were entirely too slow. Now, just a bit about Mr. Hagelin. He did what is best described as a "hysteron proteron." That's a four-bit word from the Greek meaning to do a thing ass backwards. ((Audience laughs. He chuckles.)) I mean that usually you go into cryptographic work and then you have a nervous breakdown. He did it the other way around. He had a nervous breakdown, and it was during his recovery that he invented this machine. ((Audience laughs.)) He made nearly two million dollars—U.S. dollars—from his invention. That's not at all a poor sort of "hysteron proteron" if you're going to do one. ((Audience laughs again.)) Here's a picture of Hagelin's very first machine. No, that's the…That's the one that we finally used. I think it…Oh, no. Take that away please. Take that back. Take both of them back. ((Audience laughs.)) I took out that slide and forgot. Just leave the lights off please. I brought that first…very first model with me and you can see it after class. It was a present from Mr. Hagelin for my museum. From the first prototype, he built better models and he interested the Signal Corps in them. As a consequence, we built in

America for World War II a six-wheel Hagelin machine, which many of you no doubt know as Converter M-209. We built a large number of them. Over 110,000 in fact. They were used by the Army, the Navy and the Marine Corps.

Now…No, go back please. ((He pauses.)) That's it. Leave that one there. This is a picture of one of our M-209s as modified by a couple of our GI's in Italy. The M-209, as you…many of you no doubt know, has no printing mechanism. And you know how resourceful GI's can be. By scrounging parts here and there, they improved their machine to make it a printing model. See the keyboard over on the left? And there's the printing mechanism. Inside the cover, they pasted a cartoon of a couple of GI's getting ready to test a homemade still for the production of you-know-what. The caption at the bottom of the cartoon says, "Yes, but will the god-damned thing work?" ((Audience laughs; Dr. Friedman chuckles.)) Mr. Hagelin continued to improve his machine, and has produced several models which print not only the plaintext but also the cipher text. And some of them have electrically-powered keyboards with associated driving mechanisms. However, all of these models have a serious weakness. ((He pauses.)) The weakness is that when two messages are in depth—that is, when they are enciphered by the same keying sequence—they are solvable.

Now for a quick review of the development of what we call electrical rotor machines. The first one I show, also a product of Mr. Hagelin in Stockholm, was not a real rotor device of the type we use today, but I don't want to go into details. I merely want to show the device, which is now, as you see, connected to a Remington typewriter. So that instead of writing down letters one by one, you can make much more speed by having a printed record. Up to that time, devices of this sort were only of the lamp indicator type. You'd press a key, a rotor would move, a light would light, but you'd have to write down the letter that flashed on the light bank, and then press a key for the next encipherment.

The next forward step was taken when Hagelin made the printing mechanism an integral part of the machine. Here's the keyboard. The printing mechanism is inside the box. And now the whole assembly is very much smaller and more compact.

Now I show you a model of a German machine—the Enigma, the commercial model—which was available until Hitler came into power. It comprised a keyboard, a light bank, a set of circuit changers called rotors, and a dry cell for power. In this case, the enciphering and deciphering

circuitry is more complicated. The current goes from a keyboard to a contact on a fixed entry plate or stager, and then through the stepping rotors to a reflector or reversing plate, which sends the current back through the cipher rotors—but over a different path to one of a bank of lights. The current thus goes through the rotors twice, which complicates things a good deal. Each time a key is depressed, at least one rotor steps forward and changes the circuits. In World War II the Germans used a modification of the Enigma, but they lost the war nevertheless. ((Audience laughs.))

Now, I want to go directly to the American developments in rotor machines. First, I show a picture of the late Mr. Edward H. Hebern, a Californian, who seems independently to have thought of rotor machines. I asked Mr. Hebern one day how he happened to get started on such things. And he said, "Well, you see, I was in jail." I said, "In jail? What for?" He said, "Horse thievery." I asked him, "Were you guilty?" Whereupon he said, "The jury thought so." ((Audience chuckles.)) It was while he was in jail then that Mr. Hebern conceived the idea of a cipher machine. Here is his very first model. It is possible that he built it as an item of occupational therapy while in jail. ((Audience laughs.)) It has a keyboard, a left-hand stator—that is, a ring of 26 stationary contacts arranged in a circular fashion to one of the current…to one of which the current goes when a keyboard key is depressed—a rotor of 26 points and an exit stator of 26 contacts on the right side. It is important to note that there was no reflector rotor. This…The type here is what we call "straight through" rotor machine. You press a key and the lamp lights. There was, as you see, just one rotor in this model, which he built in 1922 for the use of the Ku Klux Klan. Here is the first prin…((Audience laughs.)) Here is the first printing model made by Mr. Hebern—still a one-rotor machine with a keyboard and now an electric typewriter connected thereto. This shows his next step of development. Now we have three rotors in cascade. That, too, was a very important step. The cascading effect was a great advance in connection with rotors.

Here I show his next development: a rotor machine with five rotors. There's an interesting story connected with that model. The Navy thought this Hebern model a suitable machine. And they had for crypto developments at that time a large sum of money for those days—seventy-five thousand dollars! They proceeded to negotiate with Mr. Hebern. I was asked by the president of the Naval Board who had been appointed to study the machine to give him my personal opinion of its security. I persuaded the War Department to purchase one machine from Mr. Hebern for my study. The whole of my outfit then consisted of myself and a World War I veteran—an ex-prizefighter with crossed eyes, pug nose and cauliflower ears. The only thing he could do was to operate a

typewriter accurately. Everything else was up to me. I studied that Hebern machine for three or four weeks without even a glimmer of an idea for a solution.

Suddenly one came to me. I tried it out and found it worked pretty good. Whereupon I went over to the Navy section, which was then in charge of a Lieutenant Strubel—now Vice Admiral Strubel, retired—with an enviable service record. I said to Strubel, "Lieutenant, I don't think that machine is quite as safe as you think it is." He said, "You're nuts." I said, "Does that mean you challenge me?" ((Audience laughs.)) He said, "Yes." So I said, "I accept." He asked, "What do you want by the way of…in the way of messages?" I said, "Oh, about ten messages put up on your machine with your own special rotor and wirings." He gave me the ten messages, and I worked on them until I got to a place one day at the close of business when I had reduced the text of the first line of one of the messages to its simplest terms. I knew only which letters were the same in that line, but I didn't know what the letters actually were. Let us say, for instance, that the third, the fourteenth, the nineteenth, and the twenty-fifth were the same, whatever they were. The ninth, the twelfth, the eighteenth, twenty-fourth were the same and so on. That's all I had when I left for home that evening.

We were going to some sort of a party, but these identities were apparently deeply embedded in my subconscious. As I was tying my black tie, it suddenly came to me…And I can't tell you to this day just how or from where. But the whole line of text fell into place with all repetitions in the proper place: "President of the United States." I could hardly wait to get to the office next morning when, to my intense gratification, I found that my subconscious was correct. I reconstructed the ten messages, turned them over to Lieutenant Strubel. And there was a considerable amount of excitement after I showed him how I had reasoned out the solution. I don't know whether he understood it. ((Audience laughs.)) The Navy Department cancelled the order that they had placed.

The Hebern Company, which had been selling stock at two dollars on the basis of great prospects of selling many machines to the U.S. Navy, suffered a financial disaster ((audience laughs)), and went to pieces. Mr. Hebern, trying to resuscitate what he could from his unfortunate encounter with an unknown cryptanalyst, bought Hebern stock in the southern part of California at forty cents and sold it to people in the northern part of the state at about two dollars. ((Chuckling heard.)) The California Blue Sky laws didn't like that sort of conduct, and Mr. Hebern spent another year in jail ((audience laughs)), giving him lots of time and opportunity to think up improvements to his machine. ((More chuckling heard.)) Despite my solution we thought that the Hebern principle was still a good one. And,

because the money was available, the Navy went ahead with Mr. Hebern after he got out of the clink. He built another model. And soon after its delivery Mr. Hebern…Oh, that represents that…the first few lines of that message. Well, you can see in the…"Resident of the United States." The "P" and "R" belong to the tail end of what goes before; and there were three letters in front.

Now, let's see the next slide. Yeah. This is the machine he built when he got out of the clink. He built another model, and soon after its delivery Mr. Hebern naturally wanted to get paid for it. But there was just one hitch. The machine wouldn't work. When this was pointed out to him, he said, "Show me where it says in the contract that it has to work." ((Audience laughs.)) And when they couldn't, he was paid off. ((More laughter heard; Dr. Friedman chuckles.)) The Navy then decided that they had had enough of Mr. Hebern and went into research and development themselves, establishing in Washington a laboratory in what was then called the Navy Yard. Years later, the Hebern heirs brought suit in the United States Court of Claims against the United States for fifty million dollars, which was settled only a couple of years ago at a considerable discount—thirty thousand dollars—just to get him off their necks.

Now for a few words about Army developments in rotor type crypto machines. After the debacle I told you about, we, in the Signal Intelligence Service in the Office of the Chief Signal Officer in Washington, had the cooperation of the Signal Corps Laboratories in developing a machine for the Army. Here's a picture of it. ((He pauses.)) These machines worked. But even before ten of them had been produced, we had hit upon a new principle for control of the rotor stepping. I tried my very best to get my division chief to change the development right there and then—and shift to the new type of control. I was practically thrown out of his office—I won't say on what part of my anatomy—on my third try, with the remark, "Go back to your den. You inventors are all alike. A new and better idea every day. If we listened to you inventors, we'd never get anything out." So we had to put the idea on ice—that is, in secrecy for a while.

Now, about that time, the Navy had its Mark I ECM—or Electric Cipher Machine—developed and built without any help from Mr. Hebern. There wasn't any collaboration in those days between Army and Navy cryptologists. We didn't even know that such a machine had been built by the Navy. Each service went its own way. When there came a change in command in the Navy Code and Signal Section, the new head decided that the security of the Mark I ECM wasn't good enough, and he wanted some help from the Army if he could get it. He came to see me one day and told me they were in difficulty and needed new ideas. Did we have

any? I said, “Hmm, well, we’ve got a good idea, but it’s secret.” He asked, “What do you or I have to do to get it released so that you can tell me?” I told him, “I’ll try to get permission from the Chief Signal Officer,” which I proceeded to do. I mention this specifically and ask that you believe that this was the situation in those days. There were Army cryptologic secrets and Navy cryptologic secrets—and never did the twain meet.

When I told the Chief Signal Officer what the Navy wanted, he promptly said, “Of course! Let them have it.” So we told the Navy about a new idea for rotor control. We showed them the circuitry involved. They liked it. And by joint action, a large number of new machines for the Navy and for the Army were built by the Teletype Corporation—a very competent organization. The machines used the Army crypto principles, and they were highly successful. Here’s a picture of the Mark II ECM—Navy terminology; or SIGABA—Army terminology. If it hadn’t been for the fact that we got together before we became belligerents in World War II, Army-Navy secret intercommunication would have been extremely difficult. The ECM-SIGABA came into use just in good time and it was used with great satisfaction on *both* the Army and Navy sides during World War II.

I might add in closing that incident, that to the best of my knowledge this is the only gadget that was withheld from our British allies throughout World War II. They knew we had a machine of this character. And although we knew all about their type of machine—in fact, the Navy was using it for communication with the British—it was U.S. policy at the highest level in both the Army and Navy to withhold our machine from the British.

I think it would be nice if there were time to explain the crypto principles of the ECM-SIGABA. But suffice it to say that we know of no case of solution of messages enciphered by it. And it is still in service as a high-grade offline machine. During its use in World War II, there was one possible compromise, which raised quite a storm when it was discovered that some Frenchmen had liberated a U.S. Army truck and trailer—the latter carrying all the 28th Division’s Headquarters cipher machines and material. But the stuff were soon found where it had been dumped in a nearby river by the Frenchmen—who wanted only the vehicles, not their contents.

If so, it was one which caused the signal officer and other officers to be tried by court martial. We had, and still have, very strict rules indeed about safeguarding this gadget and others. ((He coughs.)) And in mentioning this point, I should say that we weren’t worried by the fact…by the thought that our messages could be read if the Germans would capture one. We were worried by the thought that they would learn how

good it was and would copy it—thus cutting off our COMINT.

I can hardly refrain from telling you one of the funny things about our not giving the machines to the British when they needed and wanted it so desperately. I mentioned the strict rules about safeguarding: who could see the thing, who could service it, and so on. And we saw to it that these rules were strictly enforced. But there came a time in North Africa when all our maintenance men were knocked off. There was nobody to service the machines. However, a very skillful British RAF officer, an electrical engineer, was pressed into service and he maintained our SIGABAs there for a while. I'm sure you won't be astonished to learn that when he got back to London, he built for the RAF a machine based upon ECM-SIGABA principles.

Now we come to the development of cipher machines for protecting teleprinter communications—the need for which had been recognized even during World War I. In 1919, for example, the AT&T Company engineers in collaboration with the Signal Corps devised this modification of the then-standard printing telegraph machine to make it a printing telegraph cipher machine, using circular key tapes of random characters. Great faith was placed in the machine, but was not put into use until the war was over. By that time, I was back from France. We joined the Riverbank Laboratories, and accepted a challenge to solve this kind of cipher system. It's too long a story to go into right now, but as a result of the solution, the Army dropped the project. In a way, I think it was too bad because when we had a desperate need for teleprinter ciphering in the early days of 1942, we actually had nothing except this thing. The big trouble, of course, was the production and distribution of these key tapes. And it is still a problem which is with us. Here's a early model of the machine for making key tapes, I hope. Yes, that's right. We improved such machines very greatly in the next year or two so that we could produce hundreds of thousands of good key tapes in a hurry.

This is a rotor machine—the SIGCUM—which the Army developed in 1942-43 and which was used very successfully by both services to encipher teletype communications. It uses not perforated tapes but rotors, which step in an erratic fashion. Every once in a while when we discovered a new cryptanalytic technique, we found that the SIGCUM had weaknesses which could be exploited. Whereupon we would proceed to tighten up things by changes in the method of usage or the method of stepping the rotors and so on. The machines are still in use—some of them—doing valiant service because we were able to incorporate more and more improved features in (B% them).

Now, a few words about certain other types of ciphering apparatus. For

example, it is necessary to send with security weather and situation maps. The generic name we gave to machines for enciphering facsimile was cifax. We also had machines for enciphering telephone conversations—machines to which we gave the generic name ciphony equipments. The Bell Telephone Company in collaboration with engineers from the Signal Intelligence Service and the Signal Corps developed a very high-grade ciphony system which became known as SIGSALY and which was extremely successful. But each terminal, of which there were seven, cost over a million dollars.

The professional cryptologist is always amused by the almost invariable reference by laymen to *the* German codes. So, as I told you before, hundreds of cipher systems are in simultaneous use in our defense communication services. You not only have to have different kinds of systems to meet specific types of communication, but you have to divide up the traffic for two reasons. First, so as not to overload one system beyond the safety limits—and so that not everybody can read everybody else's messages, even if they all have the same machine or crypto system. There was a leak in connection with the Navy success in the Battle of Midway. And it happened primarily because this last principle wasn't in effect at that time in U.S. Naval communications.

((He clears his throat.)) Keeping track of crypto material and accounting for it is a big headache. There's no way of getting around this that I know of. And it is important that the rules for the protection of the material be followed absolutely to the letter. The Japanese also had very definite and detailed instructions for accounting for crypto material. They were enjoined to burn the books, the cipher keys, the cipher table and so on. They were enjoined to scatter the ashes and then make a certificate, witnessed by a fellow officer, as to the complete destruction of the material.

But one day, one chap was observed through binoculars when he took a spade and dug a hole, dumped the code books and the tables in that hole, and poured in some water. In due time, some of our people sneaked out, dug into the hole, got out the material, brought it in and dried it. This sort of recovery of crypto material helped a great deal because it saved us an enormous amount of time and labor to reconstruct that particular code and set of tables.

I have already mentioned that the Japanese were worried about their crypto security. Their crypto systems were very complex, and they felt sure of their security. Yet, they felt that *something* was wrong. And the only thing they could imagine was that there were *spies* all around them. We read and were amused by messages requiring the commands to go

through their quarters and look under the beds and in…through all the closets hunting for spies. Of course, that wasn't the case at all. We were solving their codes and ciphers because they were not secure.

You have seen some of the important World War II developments in crypto apparatus. And I wish that there were time to show you and tell you a bit about the new ones conceived and developed and sometimes produced by the NSA. In general, the trend has been toward these things. First, making the machines more manageable as to size and weight by miniaturization, the use of transistors, and other solid state components—and by better packaging. Second, by making the machines more secure by incorporating better and more advanced crypto principles. And third, by simplifying the procedures. The aim of simplification is accomplished wherever practicable by eliminating as many features and procedures which, because of operator's errors, lead to crypto security weaknesses. That is, we've been trying to make the machines as nearly automatic and as nearly foolproof as possible so as to eliminate weaknesses caused by human error. We must take into account the fact that the machines have to be operated by human beings, who occasionally make mistakes and who are prone to errors of omission and (B% commission). Experience has proved in the past that it has been these errors that have made solution on a regular basis possible.

You understand, I'm sure, that we depend for crypto security not on keeping the construction or design of the machines deep secrets. This means that the machines must be based upon crypto principles such that, even if the machines fall into enemy hands by capture or otherwise, without possession of the exact key for the day/the exact key for the period/or for each individual message itself, the enemy can never learn by cryptanalysis the contents of any messages. Or at least he can't for a great number of years. At the same time, there is a real point in keeping the machine itself in a classified status as long as possible.

Because in the case of a well-designed crypto apparatus, if you don't know what the machine looks like to begin with, or its general principles of ciphering, you can't even make a start at cryptanalysis. Or to be more accurate, it will take a considerable length of time and more or less involved study to ascertain what you must know before you can start an attack on the messages with some hope of success. In a nutshell, then, we keep the machines in a classified status as long as possible: first, in order to delay the enemy's real attack on the traffic. And second, to prevent a potential enemy from duplicating the machines and turning them…those weapons against ourselves.

I'm sorry that I can't show you pictures of some of our new machines. And

anyhow, it wouldn't do much good unless I had time to explain specifically what they are for and how they work. I will say, however, that we now have machines for literal communications such as the KL-7, which has a keyboard and prints the cipher text. It uses any 24-volt source. Several thousand of them have been issued to our NATO allies. We have machines for online and offline teleprinter ciphering. And we have one online synchronous teleprinter cipher system with link encryption. That is, so far as enemy intercept is concerned, it is impossible to tell when the circuit is idling and when a circuit…when a message is being transmitted.

Next, we have new and better ciphony systems in machines for protecting telephone communications. I told you a bit about SIGSALY of World War II days—each terminal of which cost over a million dollars. But we now have cipher machines of equal security which are much, much smaller and cost a mere thirty thousand dollars apiece. Then we have new cifax machines for protecting facsimile transmissions. Nowadays , we place emphasis on telephone security devices and systems and on automatic teleprinting systems. The days of hand-operated devices is over…are over. And those of semiautomatic offline cryptographic machines are drawing to a close. And last to be mentioned, NSA crypto engineers are doing development work on what we call "civision" systems: enciphered television, which will doubtless come into use with a few years.

But with all these modern improvements, I don't think the day has yet dawned when it can be said that human factors that make for crypto insecurity have been entirely eliminated. Perhaps it's true that, at the moment, COMSEC technology can be said to be ahead of COMINT technology. But it is possible that the COMINT gap can be closed. In short, it is the age old battle between armor and armor-piercing projectiles. In the meantime, communicators must keep their guard up and enforce the rules supplied them for operating their crypto equipments.

Let me remind you, first, that the establishment and maintenance of communications security is a responsibility of command. Second: that there aren't any shortcuts to achieving communications security. And third: that the rules of communications security must be followed to the letter by everybody connected with COMSEC—but most especially by crypto operating personnel. If these reminders are followed, the chances are good that you won't learn your COMSEC laws by accident.

If there is any last word or impression that I would like to leave with you, let it be that, in my opinion, COMSEC, though less spectacular…Turn off the lights…Ah, turn on the lights. Thank you. Ah, in my opinion, COMSEC, though less spectacular and less interesting than COMINT, is the more important of the two faces of the cryptologic coin. There are two

reasons for this opinion. The first is, that in the conduct of modern large-scale military operations—ground, sea, air, and paramilitary—COMSEC is of the highest importance because without secure communications, nearly every such operation is doomed. The second reason is one that is not so obvious. It is that your COMINT successes will soon be eliminated unless the communications over which the traffic and the final results must pass to those who can use them are secure.

Therefore, COMSEC is doubly important. First, to protect our own plans and movements; and second, to protect our COMINT product and sources. I'd therefore like to present for your consideration and rumination the following statement of which I'll…of what I'll immodestly call "Friedman's Law"—something patterned after Parkinson's Law. Your cryptologic coin, like any other coin, has two faces. If you're up against equal or even superior forces and if the COMINT face of your coin is bright and shiny, your chances of winning are good—maybe at times excellent. But if you let the COMSEC face of your coin become tarnished and dull, you'll sure as hell lose.

Thank you for your patience in listening to my rather lengthy discourse and for your courtesy in paying such careful attention to what I have presented for your information. Those of you who care to examine some of my exhibits are invited to come up to the table. And we can look at them as long as you wish. Thank you very much. ((Audience applauds.)) ((TR NOTE: Audio ends at this point.))

////////////////////////////////////End of transcript////////////////////////////////////